STATEMENT BY
ROBERT M. JACKSTA
EXECUTIVE DIRECTOR, BORDER SECURITY AND FACILITATION
OFFICE OF FIELD OPERATIONS
CUSTOMS AND BORDER PROTECTION

Hearing before the House Committee on Transportation and Infrastructure
Subcommittee on Coast Guard and Maritime Transportation

OCTOBER 6, 2004

Good morning Chairman LoBiondo and Members of the Subcommittee. Thank you for this opportunity to update you on the progress U.S. Customs and Border Protection has made in further strengthening U.S. seaports and protecting our trade lanes and the global trading system--the very means of global trade--through revolutionary supply chain security initiatives.

Trained CBP Officers, technology, automation, electronic information and partnerships with the trade and foreign governments are concepts that underpin CBP's port security and anti-terrorism initiatives. These concepts expand our borders and reinforce the components of our layered defense to better secure maritime trade. These layers are interdependent and are deployed simultaneously, to substantially increase the likelihood that weapons of terror will be detected. Today, I would like to focus on how this layered defense works with regard to maritime security.

Working with industry, we set out to devise a strategy to secure the primary system of global trade--containerized shipping—without grinding global trade to a halt.

Starting in late 2001, U.S. Customs, now U.S. Customs and Border Protection, developed and began implementing a strategy to increase security against the terrorist threat, but one that would also actually facilitate the movement of trade.

We did this by implementing four interrelated initiatives: the 24-Hour Rule, the Container Security Initiative (CSI), the Customs-Trade Partnership Against Terrorism (C-TPAT), and the National Targeting Center, a primary user of our Automated Targeting System (ATS).

Every one of these initiatives is designed to make our borders smarter –and to extend our borders by pushing our security measures out beyond our physical borders so that our ports and our borders are not the first line of defense. Moreover, these initiatives are designed to meet the twin goals of increasing maritime security, but doing so without choking off the flow of legitimate trade.

These initiatives make use of technology, advance information, extended border concepts, and partnerships to achieve our goals.

National Targeting Center (NTC)

To effectively secure sea, land and air ports of entry, CBP must have access to electronic cargo information in advance, the automation technology to manage this information, and experienced personnel to evaluate and apply this information. Our National Targeting Center achieves these goals through the mandate that we obtain advance electronic information on all cargo shipped to the United States 24 hours *before* the cargo is loaded at foreign seaports.

The National Targeting Center has established a range of liaisons with other agencies responsible for securing U.S. borders. For example, CBP and the Coast Guard have exchanged liaison officers at the NTC and the Intelligence Coordination Center at the National Maritime Information Center to address and coordinate on issues related to vessels of interest and maritime threats. Another example involves the Food

and Drug Administration, who commenced around the clock joint targeting operations at the NTC on December 11, 2003 in support of the Bio-Terrorism Act.

Automated Targeting System (ATS)

CBP's Automated Targeting System (ATS) is a functioning and operational tool that permits the National Targeting Center to process advance information and focus CBP's inspection efforts on potentially high-risk transactions. In the cargo environment, the targeting system analyzes electronic data related to the individual shipments to profile and rank them in order of risk.

Although ATS inputs go well beyond advance manifest information, the scope and reliability of the cargo information currently received under the 24 Hour Rule is reinforced by the Trade Act Final Rule published on December 5, 2003. This Rule mandates advance electronic cargo information inbound and outbound for all modes of transportation.

All oceangoing cargo containers that are identified through CBP's ATS as posing a potential terrorist threat are inspected, usually with large-scale imaging equipment and radiation detection devices, on arrival at U.S. seaports, if not before—which takes me to the Container Security Initiative.

Container Security Initiative (CSI)

The Container Security Initiative (CSI) came into being as a direct result of the events of September 11. The purpose of this initiative is to extend our nation's zone of security. Essentially, CBP assesses the risk of oceangoing containers headed for the United States *before* it is loaded on a vessel in a foreign port and *before* that vessel is bound for our seaports. With our host nation counterparts, CSI permits a prescreening

of high-risk containers *before* they are loaded on board vessels destined to the United States. With the prescreening of high-risk containers, the CSI program secures the movement of legitimate trade as well as facilitates the movement of trade by using time prior to the landing of the container for inspectors, rather than after arrival. Thus, the normal lag time for a container awaiting loading is used to enhance both security and trade facilitation. Various countries with ports shipping the greatest volume of containers to the United States have been committed to join CSI. CBP has CSI agreements with 20 nations; and we have CBP targeting teams operational at 26 foreign ports.

Customs – Trade Partnership Against Terrorism (C-TPAT)

After September 11, CBP approached the trade community to devise a joint strategy to protect the global trading supply chain. The Customs – Trade Partnership Against Terrorism (C-TPAT) was developed to meet this need.

Some of the basic tenets of C-TPAT are:

- Strengthening and enhancing supply chain security.
- Developing a security conscious environment throughout the entire commercial process;
- And engaging trade associations and international organizations in developing global security standards.

Participation in C-TPAT has grown; currently there are over 7000 private sector partners. Today, CBP teams are in the process of verifying the information submitted by the C-TPAT participants to ensure that appropriate measures are in place to help secure the supply chains.

CBP is also working with the industry to have a smart and secure container that prevents and deters tampering, alerts government and trade when tampering does occur, and is inexpensive.

Non-Intrusive Inspection (NII) and Radiation Detection Technologies (RDT)

Non-Intrusive Inspection Technology (NII) and Radiation Detection Technology is another cornerstone in our layered strategy. Technologies deployed to our nation's sea, air, and land ports of entry include large-scale X-ray and gamma-imaging systems as well as a variety of portable and hand-held technologies. CBP is also moving quickly to deploy nuclear and radiological detection equipment, including Personal Radiation Detectors (PRD's), Radiation Portal Monitors (RPM's) and Radiation Isotope Identifier Devices (RIID's).

A portion of these large-scale systems are deployed to seaports on both coasts and the Caribbean. CBP has also initiated the deployment of Radiation Portal Monitors in the maritime environment with the ultimate goal of screening 100% of all containerized imported cargo for radiation.

This equipment, used in combination with our layered enforcement strategy, allows for CBP to screen shipments rapidly for radiological weapons of mass destruction. At the same time we are working with stakeholders to ensure that radiation screening does not significantly impact operations within a port.

Operation Safe Commerce (OSC)

Customs and Border Protection continues to be a partner in the Department's Operation Safe Commerce (OSC) program. This congressionally funded initiative provides allocation of resources to fund pilot projects to enhance maritime security

through technology and enhanced business practices. The ports of New York/Newark, Seattle/Tacoma and Los Angeles/Long Beach have been selected to participate in Operation Safe Commerce. The first phase of this program is coming to completion over the next several months. There is additional money allocated to OSC, and CBP plans to have substantial input into the project.

Conclusion

Customs and Border Protection has led and implemented maritime security initiatives in partnership with the private sector and other U.S. Government agencies. Our most important partner in maritime security is the U.S. Coast Guard. CBP participates in various multi-agency working groups addressing maritime security issues; namely, Operation Safe Commerce and implementation of the Maritime Transportation Security Act of 2002. These efforts focus on Cargo Security Measures, Maritime Domain Awareness and the development of the National Maritime Security Plan, under the direction of the Coast Guard.

Mr. Chairman, it is important we have a sound contingency plan in place in the event of a terrorist attack involving our maritime system.

One of the primary reasons for implementing the maritime security strategy I have described is to develop a system that will prevent and deter exploitation by global terrorists. Another important reason is to have a sufficient security system already in place so that, if there is a terrorist attack involving maritime trade, the Department of Homeland Security, after assessing the situation, can restart the movement of trade to the United States without a prolonged shutdown of U.S. seaports.

We now have in place an automated targeting system that, with the 24-Hour Rule, allows us to evaluate all cargo containers destined for U.S. seaports and to identify those that pose a terrorist risk. Currently, the Container Security Initiative is operational at 26 of the largest ports in terms of volume of shipments to the United States. Similarly, C-TPAT has evolved to include more than 7,000 private-sector partners, implementing security processes and procedures – which we have begun validating – back to the container's point of origin.

Given these security measures and our collaboration with the U.S. Coast Guard, and other parts of DHS, I believe that we are working toward a maritime security strategy that will allow DHS to restart the system with minimal disruption, even after a terrorist incident.

I believe CBP has demonstrated and will continue to demonstrate its leadership and commitment to maritime security efforts, and we anticipate that working together we will further these efforts.

Thank you again, Chairman LoBiondo and the Members of the Subcommittee for this opportunity to testify.

I would be happy to answer any questions you may have.

####